Euroconference NEWS
L'INFORMAZIONE QUOTIDIANA DA PROFESSIONISTA A PROFESSIONISTA
Direttori: Sergio Pellegrino e Giovanni Valcarenghi

Edizione di mercoledì 19 Febbraio 2020

DIRITTO SOCIETARIO

Responsabilità amministrativa degli enti e cybersecurity

di **Cristiano Moretti, Davide Albonico**

In data 20 novembre 2019 è stata pubblicata **sulla Gazzetta Ufficiale n. 272** la **L. 133/2019**, che consta di sette articoli e che ha recepito in toto il **D.L. 105/2019** intitolato ***"Disposizioni urgenti in materia di perimetro di sicurezza nazionale cibernetica"***.

Nell'articolo 1 viene istituito e definito il ***"perimetro di sicurezza nazionale cibernetica"***, con la specifica **finalità di *"... assicurare un livello elevato di sicurezza delle reti, dei sistemi informativi e dei servizi informatici delle amministrazioni pubbliche, degli enti e degli operatori nazionali, pubblici e privati****, da cui dipende l'esercizio di una funzione essenziale dello Stato, ovvero la prestazione di un servizio essenziale per il **mantenimento di attività civili, sociali o economiche fondamentali** per gli interessi dello Stato e dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio, possa derivare un pregiudizio per la sicurezza nazionale"*.

A seguire, il **comma 2, lettera a)** dello stesso articolo delinea i **destinatari dalla norma** sulla base delle **funzioni svolte** o dai **servizi resi** dai medesimi, individuando le seguenti condizioni:

1. il **soggetto eserciti una funzione essenziale dello Stato**, ovvero assicuri un servizio essenziale per il mantenimento di attività civili, sociali o economiche fondamentali per gli interessi dello Stato;
2. **l'esercizio di tale funzione** o la prestazione di tale servizio **dipenda da reti, sistemi informativi e servizi informatici dal cui malfunzionamento, interruzione, anche parziali, ovvero utilizzo improprio possa derivare un pregiudizio per la sicurezza nazionale**.

I destinatari della norma con **cadenza almeno annuale** devono **predisporre/aggiornare un elenco delle reti, dei sistemi informativi e dei servizi informatici di rispettiva pertinenza**, comprensivo della relativa architettura e componentistica, da **trasmettere alle autorità competenti** contestualmente individuate.

La specifica individuazione dei **soggetti** e dei **criteri** per la **formazione degli elenchi** verrà

emanata con un **Decreto del Presidente del Consiglio dei Ministri** entro **quattro mesi dalla data di entrata in vigore** della legge oggetto di disamina.

Il **comma 3 dell'articolo 1** stabilisce che con analogo **provvedimento**, entro **dieci mesi dalla data di entrata in vigore della legge**, verranno definite le **procedure di notifica alle autorità competenti degli incidenti aventi impatto sulle reti, sistemi informativi e servizi informatici** di cui sopra, nonché le **misure volte a garantire elevati livelli di sicurezza degli stessi** e quelle relative, tra le altre, alle politiche di sicurezza, alla struttura organizzativa, e alla gestione del rischio, all'integrità delle reti e dei sistemi informativi e alla protezione fisica e logica dei dati.

Coloro che ricadono nel perimetro di sicurezza nazionale sono tenuti al **rispetto di una serie di obblighi informativi e procedimentali**, e verranno **sottoposti ad attività di ispezione e vigilanza di specifiche autorità**. È inoltre previsto un articolato **sistema sanzionatorio per i casi di violazione degli obblighi** previsti.

Si ricorda a tal proposito la rilevanza strategica del **Centro di Valutazione e Certificazione Nazionale**, che è stato all'uopo istituito presso l'**Istituto Superiore delle Comunicazioni e Tecnologie dell'Informazione (ISCTI) del Mise** con decreto di quest'ultimo datato **15.02.2019**, e che dovrà **assicurarsi delle garanzie di sicurezza e dell'assenza di vulnerabilità** di prodotti, *hardware* e *software*, destinati a essere impiegati sulle reti, sui sistemi informativi e servizi informatici.

Al riguardo, il **sesto comma dell'articolo 1** prevede l'istituzione di un **meccanismo finalizzato ad individuare una gestione degli approvvigionamenti più controllata e sicura** per i soggetti inclusi nel perimetro di sicurezza nazionale che intendano procedere **all'affidamento a terzi di forniture di beni e servizi di *information and communication technology* (ICT)** destinati a essere impiegati sulle reti, sui sistemi e per i servizi rilevanti.

Tale legge segue ad affianca la precedente **L. 56/2012**, a mente della quale vennero **introdotti poteri speciali sugli assetti societari nei settori della difesa e della sicurezza nazionale**, nonché per le **attività di rilevanza strategica nei settori dell'energia, dei trasporti e delle comunicazioni**, ed interessa (**articolo 3**) anche **i soggetti che operano sulla base delle disposizioni già previste in materia di reti di comunicazione elettronica a banda larga con tecnologia 5G** ampliando l'esercizio dei poteri speciali (la c.d. ***golden share*** introdotta con **D.L. 21/2012**), consistenti anche nell'effettuazione di **stringenti verifiche sulle eventuali vulnerabilità presenti sulle reti e i sistemi basati su tale tecnologia**. Tale verifica, svolta dal **CVCN**, può comportare peraltro *"la sostituzione di apparati o prodotti che risultino gravemente inadeguati sul piano della sicurezza"*.

Con **l'articolo 4** il legislatore ha inteso coordinare l'attuazione del **Regolamento europeo 2019/452** sul controllo degli investimenti esteri, con **l'**articolo 2, comma 1-ter, D.L. 21/2012, dotando la **Presidenza del Consiglio dei ministri e le altre amministrazioni competenti** della possibilità di **applicare con immediatezza la disciplina dei poteri speciali con riferimento ad infrastrutture o tecnologie critiche attualmente non comprese nel campo di applicazione** degli

articoli 1 **e** 2 D.L. 21/2012.

Di notevole importanza poi il **comma 11 dell'articolo 1**, il quale prevede, oltre alla **reclusione da 1 a 5 anni per le persone fisiche**, la **responsabilità ai sensi del D.Lgs. 231/2001** applicando agli **enti la sanzione pecuniaria fino a quattrocento quote** a fronte del compimento delle seguenti specifiche ipotesi delittuose:

- chiunque **fornisca informazioni, dati o elementi di fatto non rispondenti al vero, rilevanti per la predisposizione o l'aggiornamento degli elenchi di cui al comma 2, lettera b)** della legge in disamina, al **fine di ostacolare o condizionare le attività inerenti al procedimento di predisposizione e comunicazione delle reti, dei sistemi informativi e dei servizi informatici rilevanti** ai sensi della stessa legge nonché le **attività di ispezione e vigilanza in materia** (svolte rispettivamente dalla Presidenza del Consiglio dei ministri, per i profili di pertinenza dei soggetti pubblici e di quelli di cui all'articolo 29 del codice dell'Amministrazione digitale di cui al **Lgs. 82/20015**, e il Ministero dello sviluppo economico, per i soggetti privati), ovvero
- chiunque **ometta di comunicare, nei termini prescritti, i dati, le informazioni o gli elementi di fatto richiesti dalla legge**.

È di tutta evidenza come la legge in oggetto abbia espressamente previsto un **ampliamento delle fattispecie di reato presupposto** i cui settori maggiormente interessati saranno verosimilmente quelli relativi alla **produzione di energia, alla gestione di gasdotti ed acquedotti, dei trasporti e delle telecomunicazioni e quello della salute**.

Tuttavia, sarà necessario attendere l'emanazione dei richiamati provvedimenti per individuare l'esatta portata della novità normativa, l'eventuale necessità di **aggiornamento del Modello di Organizzazione, Gestione e Controllo** e, soprattutto, per circoscrivere i soggetti sostanzialmente interessati dai nuovi adempimenti.